Microsoft

Operating System

In a Windows NT Server 4.0 Environment

White Paper

Abstract

The Microsoft® Windows® 2000 Professional operating system is designed to provide users and information technology (IT) professionals with powerful new productivity capabilities and lower total cost of ownership (TCO). This paper describes the benefits of using Windows 2000 Professional in network environments running the Windows NT® Server operating system versions 4.0 and 3.51.

This document is based on features in the Beta 3 version of Windows 2000 Professional (April 1999). Readers should be aware that features in the final released version of Windows 2000 Professional might vary.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0699

CONTENTS

INTRODUCTION

Windows® 2000 Professional operating system is designed to provide end users and information technology (IT) professionals with powerful productivity capabilities and lower total cost of ownership (TCO) in environments based on the Microsoft® Windows NT® Server operating system versions 4.0 and 3.51. Windows 2000 Professional users—who have a Windows NT-based network—will experience the same features and capabilities as Windows 2000 Professional users in a Windows 2000 Server environment. Windows 2000 Professional also provides support for management, security, communications and networking capabilities by:

- **Networking and Communications**. Windows 2000 Professional provides an enhanced Network Places folder, offline folders and synchronization. Windows 2000 Professional users can more easily setup connections, including Virtual Private Networks (VPNs), to remote Windows NT 4.0-based servers. Windows 2000 also supports an enhanced type of VPN connection, called L2TP (Layer-2 Tunneling Protocol). Windows 2000 Professional is also compatible with Windows NT Server 4.0-based printers.
- **Management and Deployment**. Windows 2000 Professional is compatible with existing Windows NT Server 4.0 system policies, specifically *.pol files. Both Windows NT Server 4.0 and Windows 2000 Server supports the Microsoft Management Console (MMC), an extensible framework for management applications. Windows 2000 Professional also supports Windows NT Server 4.0-based management tools in an enhanced MMC-based form such as Event Viewer, Performance Monitor and Server Manager. Most deployment enhancements, such as the Setup Manager Wizard for creating automated installation scripts and disk image copying (“cloning”) using the System Preparation tool are fully supported in Windows NT Server 4.0-based environments. Support for Web-based Enterprise Management (WBEM) in Windows 2000 Professional or Windows NT 4.0 with Service Pack 4 makes it easier to manage desktops using a variety of management tools, such as Microsoft’s Systems Management Server.
- **Security**. Windows 2000 Professional provides compatibility with all areas of Windows NT LAN Manager-based security. Windows 2000 Professional supports the Public Key Infrastructure (PKI), which is enabled by Windows NT Server 4.0 or the Windows 2000 Server X.509 Version 3 certificate server. Additionally, Windows 2000 Professional provides encrypted file system capabilities, which are supported in Windows 2000 Server-based environments.

Accessing Network Resources

To help users find information and resources throughout their corporate networks, the Network Neighborhood folder has been replaced with the My Network Places folder. This folder includes several additional views, such as Recently Visited Places and Computers Near Me. The Add Network Place option makes it easier to set connections to other servers on the network. Also, users may rename any server connection, making it easier to find information. More specifically:

- **Computers Near Me**. In a Windows NT 4.0 Server-based environment, Computers Near Me will show workstations in the same domain, in non-domain environments, Computers Near Me will show computers with the same workgroup name, as specified in Network Properties.
- **Windows Explorer**. Displays the hierarchical structure of files, folders, and drives on the computer. It also shows any network drives which have been mapped to drive letters on the computer. It can also be used to view My Network Places, which lists other computers that are connected to your local area network (LAN). Windows Explorer, can be used to copy, move, rename, and search for files and folders.
- **Windows Shortcuts**. A shortcut to a network share or file location can be created directly on the client. Window Shortcuts (.lnk files) can be created by right-clicking a network file and dragging it onto the workstation, or by selecting the target network share and selecting **Create Shortcut** from the **File** menu.
- **My Network Places**. Network places are friendly-name shortcuts to network resources that can be used instead of drive letter mappings. The Add Network Place option makes it easier to set connections to other servers on the network. Users may rename any server connection, making it easier to find information. Users can set shortcuts to an almost unlimited number of servers. My Network Places also enhances a number of capabilities, which are fully supported in Windows NT Server 4.0-based environments. Network places can be mapped to subdirectories within a server share, rather than just to the share itself. A network place can have a path of \\server\share\dir\subdir\subdir, which makes the connection easier for the user to understand, and reduces the number of file shares that the administrator needs to create and manage.

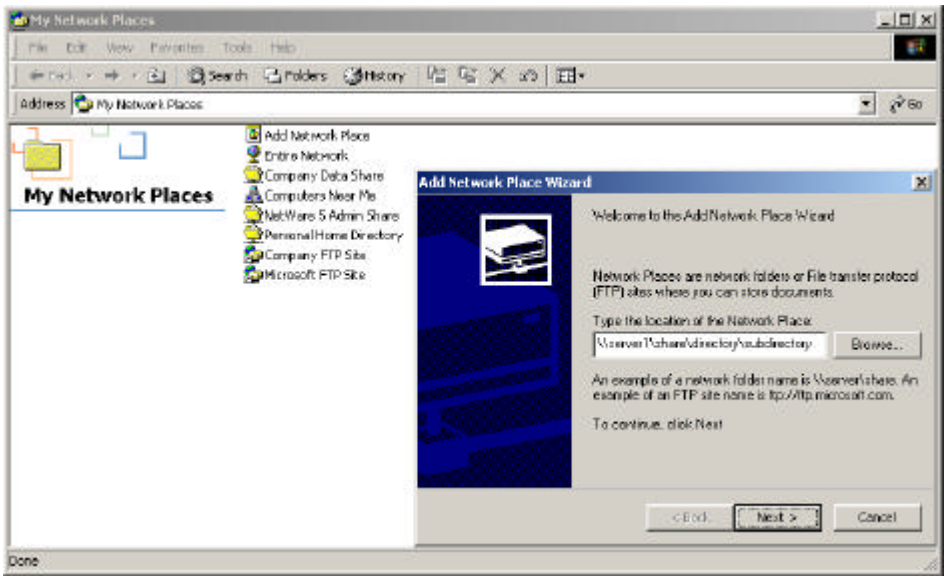

Figure 1. Windows 2000 Professional can use new features that make it easier to access network-based resources. In the above screen shot, Windows 2000 Professional is access resources on a Windows NT Server 4.0-based file share.

My Network Places treats file shares and file transfer protocol (FTP) shares as identical resources. Users do not need to go to one place for Windows networking resources, and then use a separate location for FTP resources. Additionally, My Network Places can also access files and directories over the HTTP protocol via WebDAV (the HTTP 1.1 protocol extension for Internet publishing) support.

My Network Places provides a single location for all network resource management. Computers Near Me can be used to browse the network, the Add Network Place wizard can be used to create links to file, FTP, and WebDAV shares, and printers can be mapped by using the **Connect** option.

Offline Synchronization of Server-Based Data

Windows 2000 Professional makes it easier for mobile users to take network-based files and folders offline. Users can right-click a folder or file and select **Make available offline** to make it available when not connected to the network. When offline, files and folders appear in the same *namespace*, meaning it appears as if they were still connected to the network. Files and folders set to be taken offline are visually highlighted. Users can take offline any combination of files, folders, and entire mapped networked drives and paths, for example, \\server-name\shared-resource-pathname. Offline files and folders work with any Server Message Block-based file server.

In addition, Windows 2000 Professional includes a Synchronization Manager, which provides a convenient, one-stop location for managing how and when resources are synchronized. The user can select offline files and folders as well as Web pages, e-mail, calendar information, and other applications that are written to take advantage of Synchronization Manager. Synchronization Manager provides an open API that third parties can plug in to their application or component. Based on whether the

Synchronization Manager is set on default or on customized preferences, synchronization can happen automatically.

If users choose not to use the default settings, they can set preferences for when synchronization takes place—at log off, connect or disconnect, idle, manually, scheduled, and programmatically. Different preferences can be set for individual folders or files that are managed by Synchronization Manager. For example, users may choose to synchronize offline files and folders at log on and log off, but to only synchronize Web pages every Friday at 3:30 p.m. Preferences can also be set based on connection type. For example, users can easily configure Synchronization Manager to automatically synchronize a large database file only when connected to a LAN connection and to never automatically synchronize when using a dial-up connection.

Getting Connected

Make New Connection Wizard

The Make New Connection Wizard helps administrators set up and manage remote access connections to their Windows NT-based networks. The connection wizard gives the administrator five options for remote access connections:

- **Dial-up to private network**. The dial-up to private network option creates a Microsoft Connection Manager connection to a Remote Access Server (RAS). The connections created with this option include Windows NT Domain integration, advanced security and scripting options, and can be integrated with the Connection Point Services available in the Windows NT 4.0 Option Pack.
- **Dial-up to the Internet**. The dial-up to the Internet option can be used to configure Internet settings for a LAN connection, and to create new Dial-Up Networking entries. Internet LAN settings include proxy server settings and auto-proxy discovery. Dial-up connections created with this option are similar to Windows 95, Windows 98 and Windows NT Workstation Dial-up Networking connections.
- **Connect to a private network through the Internet**. This option sets up a Virtual Private Network(VPN) connection to a remote LAN. Client-to-Server VPN connections can be created using either Point-to-Point Tunneling Protocol (PPTP) or the more secure Layer 2 Tunneling Protocol (L2TP).
- **Accept incoming connections**. This option will configure the workstation as a remote access server. Windows 2000 Professional can support only one inbound connection at a time, but that connection can be either a regular dial-up connection or a VPN connection.
- **Connect directly to another computer**. This option is used to configure the Windows 2000 Professional-based computer as either a host or guest computer for direct-cable connections.

Virtual Private Networking

Windows 2000 Professional is fully compatible with standards-based Virtual Private Network access servers such as well as the Microsoft Remote Access Server and

Windows NT 4.0 Option Pack enhancements. Virtual Private Networking creates a secure, encrypted connection between an Internet-based client, and a corporate RAS server. Once the VPN connection has been established, the remote user has encrypted access to the LAN similar to a dial-up networking connection.

In addition to Point-to-Point Tunneling Protocol, Windows 2000 Professional has built-in support for Layer 2 Tunneling Protocol (L2TP), a more secure version of PPTP, for tunneling, address assignment, and authentication. L2TP is included as a supported protocol in Microsoft Routing and Remote Access on Microsoft Windows 2000 Server.

Printing

Windows 2000 Professional fully supports Windows NT Server 4.0 Print servers. In addition to Windows NT *Plug and Print* capabilities, Windows 2000 Professional includes support for direct TCP/IP and DLC printing and mapped network printing for legacy application support. When a Windows NT print client initiates a print request, the required printer driver is downloaded from the Windows NT print server if it is not already on the client's hard disk.

Windows NT print clients can also create a remote printer served by a Windows NT print server. Each method has advantages and disadvantages. Connecting to a remote printer is easier and faster than creating one. If the Windows NT client has connected to a printer, the print job doesn't spool on the client machine, so no spool options are available. The *connected* client also cannot queue print jobs locally. Creating a printer gives the user more control, but that control is not always needed.

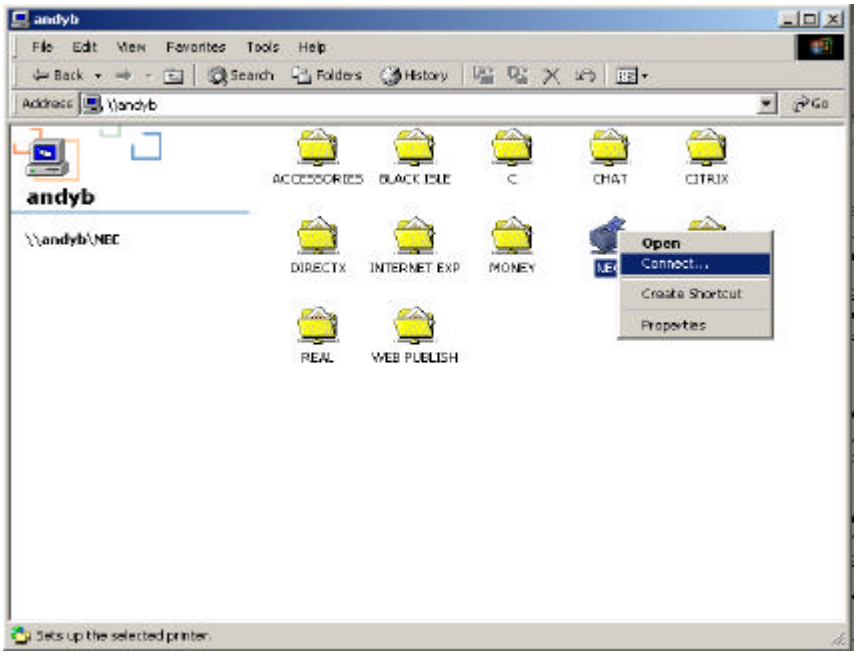

Figure 2. Windows 2000 Professional users have full access to printers on a Windows NT Server 4.0 network.

MANAGEMENT AND DEPLOYMENT ENHANCEMENTS

Desktop Management

Support for Windows NT Server 4.0-based Policies

Windows 2000 Professional is compatible with existing Windows NT Server 4.0 system policies, specifically *.pol files. Windows policies can be created and edited using the Microsoft Windows Policy Editor, Poledit.exe. Poledit.exe creates a policy file that can be used to set policies for either users or computers on the domain.

Once the policy settings have been created, the policy file needs to be saved as NTConfig.pol, then copied to the Primary Domain Controller's Netlogon share. Custom Policy Templates (.adm) can be imported into poledit and then deployed to the Windows 2000 Professional-based workstation.

Settings and Policies Distribution via Internet Explorer 5.0

As an alternative to using System Policies and a Domain Controller to administer those policies, administrators can use Internet Explorer 5.0 browser software to distribute system policies using a standard Web share location. Using the Internet Explorer Profile Manager, available with the Internet Explorer Administrator's Kit, system settings and policies can be saved to a settings file on a Web server. In addition to the default browser and Windows desktop settings, the Internet Explorer Profile manager can import .adm policy templates to manage almost any aspect of the Windows operating system. Distributing Windows settings and policies through a Web share means that workstation management is no longer reliant upon logon servers, logon scripts, or user shares. Web-based settings files are also easier to administer than policy files or mandatory user profiles.

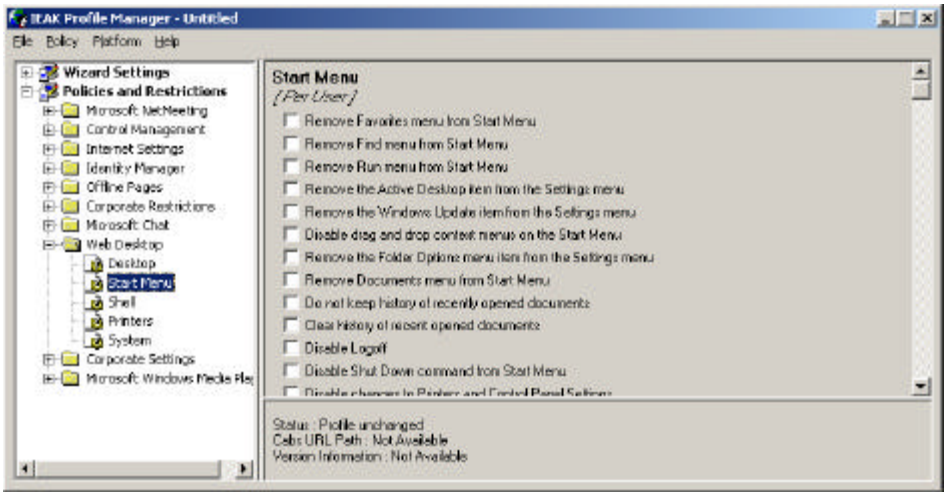

Figure 3. Administrators can manage desktop policies using a Web server as an easier to implement alternative to using system policy

Settings and Policies can be distributed through the Internet Explorer 5 browser, even if the browser is not being used. Browser-specific settings, such as the home page or security settings, also will not affect other browser applications, such as Netscape Communicator.

Enhanced Management Tools Console

Microsoft Management Console (MMC) is an extensible, common, remotable console framework for management applications. MMC does not supply any management behavior, but instead provides a common environment for Snap-Ins**,** written by Microsoft and Independent Software Vendors. Because Snap-Ins are ActiveX® controls, administrators can create and combine virtually any type of tool, either for other administrators or for users. Snap-Ins can be written not only for Microsoft tools and applications, but for third-party applications as well.

The Microsoft Management Console can be accessed and administered by a Windows NT Domain Administrator by selecting the **Action/Connect to Computer** option. The Microsoft Management Console can be installed onto a Microsoft Windows NT 4.0 server by installing the Windows NT 4.0 Option Pack.

Support for Windows NT Server 4.0-based Management Tools

Windows 2000 Professional can be remotely administered either by using MMC, or by using standard Windows NT Server 4.0 administrative tools. An administrator can integrate Windows 2000 Professional systems into an existing set of Windows NT-based management tools and procedures. More specifically:

- **Event Viewer**. The Event, Security, and Application logs of Windows 2000 Professional workstations can be accessed remotely by a Windows NT 4.0 Event Viewer. Management applications that process Windows NT-based event logs, such as Seagate Manage Exec, are also compatible with Windows 2000 Professional workstations.
- **Performance Monitor.** Performance Monitor counters on Windows 2000 Professional workstations can be viewed remotely on Windows NT 4.0 servers and workstations. Windows 2000 Professional uses the same performance counters as Windows NT 4.0.
- **Server Manager**. The Server Manager views Windows 2000 Professional systems just as it does Windows NT Workstations. All Server Manager administrative options are available for Windows 2000 Professional system. Using Server Manager, a remote administrator can view system users and shares, set in-use files and replication settings, as well as start, stop, and pause Windows 2000 Professional services.

Deployment Enhancements

Setup Manager

Windows 2000 Professional Setup Manager is a Wizard that guides an administrator through the process of creating an unattended setup file and distribution share. The enhanced script includes keys specific to installing Services for NetWare settings. The Windows 2000 Professional installation files can be copied to a Windows NT Server 4.0-based file share, and then installed either from an existing OS, or by using a network boot disk. Windows 2000 can now be used to upgrade Windows 95, Windows 98, Windows NT Workstation 3.51 and Windows NT Workstation 4.0-based systems.

Setup Manager includes the ability to:

- Choose level of user interaction, (including completely automatic)
- Set up computer name
- Set display settings
- Set network settings
- Supply drivers not on the CD-ROM
- Set printer paths
- Set commands to be run before, during, or after installation
- Set the location of the distribution share.

Disk Imaging

Windows 2000 Professional provides enhanced support for disk imaging or cloning through an enhanced System Preparation tool and stronger installation with post-installation tasks, such as configuring specific network clients. Automated installation scripts that can be used as part of the disk imaging process. In addition, because Windows 2000 Professional supports Plug and Play, disk images can be used on a wider variety of hardware platforms.

Windows Scripting Host

The Microsoft Windows Scripting Host (WSH) is a language-independent scripting host for 32-bit Microsoft Windows operating system platforms. Microsoft provides the Visual Basic®, Scripting Edition (VBScript) development system and Java Script scripting engines with the Windows Scripting Host. Microsoft anticipates that other software companies will provide Microsoft ActiveX scripting engines for other languages such as Perl, TCL, REXX, and Python.

Scripts can be run as part of a logon script, directly from the desktop, or from the command console. Because WSH is language-independent, it is possible to use existing scripts, or to create scripts with functionality available in other languages.

Windows Scripting Host allows a Windows NT 4.0 administrator to include VBScript or JavaScript code within a logon script, and add functionality beyond simple drive and printer mappings. Logon scripts can now be used to create files and shortcuts, apply rule-based logic to user logons, and to configure the Windows operating system. In addition to the object interfaces provided by Windows Scripting Host, administrators can use any ActiveX controls that expose Automation interfaces to perform various tasks on the Windows platform. For example, administrators can write scripts that automatically write entries to the registry:

```
Dim WSHShell
Set WSHShell = WScript.CreateObject("WScript.Shell")

WSHShell.Popup "Create key HKCU\MyRegKey with value 'Top level key'"
WSHShell.RegWrite "HKCU\MyRegKey\", "Top level key"

WSHShell.Popup "Create key HKCU\MyRegKey\Entry with value 'Second level
key'"
WSHShell.RegWrite "HKCU\MyRegKey\Entry\", "Second level key"

WSHShell.Popup "Delete key HKCU\MyRegKey\Entry"
WSHShell.RegDelete "HKCU\MyRegKey\Entry\"
```

```
WSHShell.Popup "Delete key HKCU\MyRegKey"
WSHShell.RegDelete "HKCU\MyRegKey\"
```

In this example VBScript is used to create and then delete two different registry keys, a top level and second level key in the **HKEY_Current_User** hive. The Windows Scripting Host does not rely on an HTML SCRIPT tag or LANGUAGE attribute to identify a script engine. Instead, it uses the extension of the script file to determine what script engine to use. As a result, the scriptwriter need not obtain a script engine ProgID. The scripting host itself maintains a mapping of script extensions to ProgIDs and uses the Windows association model to launch the appropriate engine for a given script.

Standards-Based Management

Support for WBEM

Windows 2000 Professional provides IT professionals with easier, more efficient management of computers, applications, and settings. Key among these efforts is Web-based Enterprise Management (WBEM), an industry initiative that establishes management infrastructure standards and provides a way to combine information from various hardware and software management systems. WBEM specifies standards for a unifying architecture that allows access to data from a variety of underlying technologies and platforms, and presents that data in a consistent fashion. Management applications can then use this information to create solutions that reduce the maintenance and life cycle costs of managing an enterprise network. WBEM is based on the Common Information Model schema, which is an industry standard driven by the Desktop Management Task Force.

Microsoft Windows Management Instrumentation (or WMI) is WBEM-compliant, and provides a consistent and richly descriptive model of the configuration, status and operational aspects of Microsoft Windows 2000 Professional. Used in conjunction with other management services provided in Windows 2000 Professional, WMI can simplify the task of developing well-integrated management applications, allowing vendors to provide Windows 2000 Professional customers with scalable, effective enterprise management solutions. WMI event notifications are passed to standard WBEM management tools.

WMI also allows a management application to configure a device. A management application may need to reconfigure a device based upon a driver-raised event or the data collected by the management application.

Network Security

Windows NT Server 4.0 Domain Compatibility

Windows 2000 Professional provides compatibility with all areas of Windows NT LAN Manager-based security. Specifically:

- **Windows NT Server 3.51 and Windows NT Server 4.0 Domain Logon—** Windows 2000 Professional fully supports non-Active Directory based logon authentication. Windows 2000 Professional-based workstations can be added to a Windows NT Server-based Domain and provides full compatibility with all domain services.
- **RAS Authentication Passthrough—**Windows 2000 Professional-based workstations that dial-in to Windows NT Server 4.0-based Remote Access Servers (RAS) have the same domain-integrated logon experience as Windows NT 4.0 users.
- **Server Manager Integration—**Windows 2000 Professional-based computers must be added to a domain by an administrator. Once a workstation has been added to a domain it can be administered with the same tools that are used by domain administrators on Windows NT 3.51 and 4.0-based workstations.

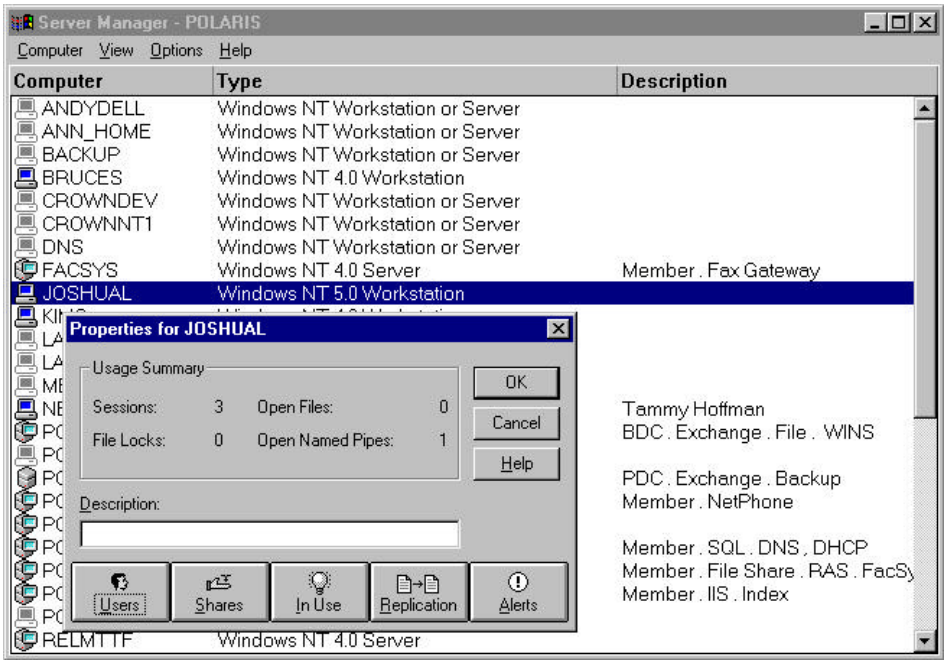

Figure 4. Windows 2000 Professional provides full support for existing Windows NT LAN Manager based authentication.

- **BackOffice Integration—**Windows 2000 Professional-based workstations are compatible with all the BackOffice applications that apply security based on a Windows NT Domain user account. Microsoft Exchange Server and Microsoft SQL Server integrated security features are available for users on Windows 2000 Professional-based workstations.
- **User Account Features—**Features of Windows NT Server 4.0 Domain

accounts, such as Windows NT Domain Groups, user profile path, home directory, logon and time restrictions, expiration dates, and RAS permissions, are fully supported by Windows 2000 Professional.

Internet Security

Public Key Infrastructure (PKI)

The separation between public and private keys in PK cryptography has allowed the creation of a number of technologies. The most important of these are digital signatures, distributed authentication, secret key agreement via public key, and bulk data encryption without prior shared secrets. The most important use of Public Keys is for digital signatures, which assure authenticity of components, including that:

- E-mail came from the sender
- E-mail cannot be viewed or edited by other users
- Applications and drivers come from known sources
- Software is protected from tampering after installation
- The identity of a remote computer is guaranteed
- Secure Internet communication is allowed
- Strong encryption is allowed, such as that needed for secure transactions.

In Windows NT Server-based environments, Internet Information Server (IIS) 4.0 includes an integrated certificate server that is tightly integrated with the Windows NT Server security model. This allows organizations to issue and manage Internet standard X.509 digital certificates. In addition to Key Management services in IIS 4.0, the Microsoft Certificate Server is included in the Windows NT 4.0 Option Pack. It provides customizable services for issuing and managing digital certificates. A Certificate Server performs a central role in the management of software security systems to enable secure communications across the Internet, corporate intranets, and other non-secure networks.

While any Windows-based platform running Internet Explorer 4.0 supports the use of Public Keys, Windows 2000 Professional goes further by providing a more robust infrastructure for Managing certificates, *trusts* with other systems, and secure storage for certificates. More specifically:

- **Managing Certificates**. Certificate Manager helps you request new public key certificates and manage existing certificates. Certificates are used to authenticate and secure exchanges of information on non-secured networks, such as the Internet. You can manage certificates for a user, computer, or service.
- **Trusts**. Windows 2000 Professional supports Transitive Trusts. Transitive Trusts are established and administered through trusted Certificate Authorities.
- **Secure Storage of Certificates**. Security certificates and Kerberos Ticket Granting Tickets are locally encrypted in Windows 2000 Professional. The ability to encrypt certificates fixes a security hole in Windows 95 where locally stored security certificates were vulnerable to Trojan horse attacks.

Local Security

Encrypted File System

An Encrypted File System (EFS) encrypts files on a hard disk. Each file is encrypted using a randomly generated key, which is independent of the user's public/private key pair. EFS resides in the Windows NT kernel and uses the non-paged pool to store file encryption keys, ensuring that they never reach the paging file. EFS is supported on a file or directory basis. Encryption and decryption is transparent to the user.

Smart Cards

Smart Cards can be used to isolate security-critical computations involving authentication, digital signatures, and key exchange from other parts of the system that do not have a need to know. This makes it more difficult to attack systems because key authentication information resides in physically different places. Smart Cards also enable portability of credentials and other private information between computers at work, home, or on the road. This eliminates the need to transmit sensitive information, such as authentication tickets and private keys, over networks.

Products such as Hewlett-Packard Praesidium Authorization Server can be used to provide secure, smart-card enhanced authentication zones on an Windows NT Server 4.0-based Domain. Smart Card readers are available from manufacturers such as Hewlett Packard, Siemens Nixdorf, Rainbow Technologies, Litronic, and Gemplus, and SCM Micro.

FOR MORE INFORMATION

For the latest information on Microsoft Windows® 2000, visit our World Wide Web site at http://www.microsoft.com/ntserver.

For the latest information on the Windows 2000 Beta 3, visit the World Wide Web site at http://ntbeta.microsoft.com